IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN RE USAA DATA SECURITY LITIGATION	Case No. 7:21-cv-05813-VB **JURY TRIAL DEMANDED**

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Vincent Dolan and Christine Mapes (collectively, "Plaintiffs") bring this Amended Consolidated Class Action Complaint ("Amended Complaint"), on behalf of themselves and all others similarly situated, against Defendant**,** United Services Automobile Association ("USAA" or "Defendant"), alleging as follows based upon information and belief, and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this class action against USAA for its: (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, Driver's License numbers ("PII"); (ii) failure to comply with industry and government regulatory standards to protect information systems that contain PII; (iii) unlawful disclosure of Plaintiffs' and Class Members' PII; and (iv) failure to provide adequate notice to Plaintiffs and other Class Members that their PII had been disclosed and compromised.

2. Plaintiffs seek, among other things, damages and orders requiring USAA to fully and accurately disclose the PII and other information that has been compromised and/or disclosed, to adopt reasonably sufficient security practices and safeguards to protect Plaintiffs' and the Class's PII from unauthorized disclosures, and to prevent incidents like this disclosure from occurring again in the future. Plaintiffs further seek an order requiring USAA to provide identity

theft protective services to Plaintiffs and Class Members for three (3) years, as Plaintiffs and Class Members are at risk and will continue to be at an increased risk of identity theft due to the disclosure of their PII as a result of USAA's conduct described herein.

3. USAA is a Fortune 500 company that provides insurance and financial services to current and former members of the U.S. military and their families.

4. Before using their services, USAA requires users to become a USAA member and create an account. Plaintiffs do not meet the requirements for USAA membership and have never voluntarily been USAA members.

5. Accordingly, Plaintiffs never voluntarily signed up for USAA membership or provided USAA with any of their PII.

6. Cyber criminals used Plaintiffs' information to open fraudulent USAA membership accounts and requested insurance quotes in their names.

7. By virtue of these cyber criminals' actions and the way USAA configured and designed its systems, Plaintiffs nevertheless became involuntary members of USAA.

8. Despite failing to meet the USAA membership criteria, USAA nevertheless allowed Plaintiffs to become USAA members and provided their PII to cyber criminals that submitted the requests for the insurance quotes.

9. On June 2, 2021, USAA provided Plaintiffs with a notice indicating that on May 6, 2021, an unidentified third-party illegally used some of Plaintiffs' information, including their names and dates of birth, to obtain auto insurance quotes from Defendant's website, www.usaa.com. Although Plaintiffs were not previously USAA members, and had never provided USAA with any PII, the auto insurance quotes Defendant provided disclosed Plaintiffs' Driver's License numbers to the unauthorized third party(s).

10. As a result, Plaintiffs have personally experienced fraud. For example, cyber criminals used Plaintiff Mapes' PII, which it obtained from USAA, to fraudulently obtain and take out insurance policies in Plaintiff Mapes' name from another third-party provider. Further, cyber criminals used Plaintiff Dolan's PII, which it obtained from USAA, to fraudulently file a claim for unemployment in his name.

11. Defendant's policies and practices allowed unauthorized third parties to intentionally target and improperly obtain Plaintiffs' and Class Members' PII through the use of USAA's online insurance quote and/or policy process (the "Data Breach").

12. Indeed, USAA intentionally configured and designed its online system to auto-populate at least responses to requests for insurance quotes with certain PII obtained from third-party data providers, including Driver's License numbers, regardless of whether those requests are submitted by USAA members or not, and to disclose that PII to whomever submitted the request. If not for USAA's intentional configuration and design of its systems, it would not have disclosed Plaintiffs' and Class Members' PII to cyber criminals.

13. The Data Breach was a direct and proximate result of USAA's flawed online system configuration and design, which unnecessarily disclosed PII to anyone who submitted a request for an insurance quote, its failure to verify whether users were even eligible for USAA membership, and its failure to implement and follow basic security procedures, such as validating the identity of insurance applicants before disclosing their highly sensitive PII.

14. Because USAA essentially left its (cyber) door wide open for unauthorized users to access and pilfer individuals' PII, Plaintiffs' and Class Members' PII is now in the hands of cyber criminals.

15. As a result, Plaintiffs and, upon information and belief Class Members, experienced *actual* identify theft, as well as substantially increased risk of future identity theft, both currently and for the indefinite future. According to the New York State Attorney General, 22,383 individuals were affected and 12,627 of them are in New York State. Plaintiffs' and Class Members' PII, including their Driver's License numbers, that were compromised by cyber criminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft.

16. Driver's License numbers can be used to file fraudulent unemployment claims, to open a new account, take out a loan in someone's name, or commit income tax refund fraud as several states (including New York) require a Driver's License number for a tax return. The cyber criminals who obtained Plaintiffs' and Class Members' PII can use this information to commit a host of other financial crimes, including identity theft (which they did), and can sell this information to other identity thieves who will do the same.

17. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to USAA's actions.

18. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, violation of the Driver's Privacy Protection Act ("DPPA"), violation of New York's consumer protection act, and injunctive relief claims.

19. Plaintiffs seek damages and injunctive relief requiring USAA to adopt reasonably sufficient practices to safeguard the PII that remains in USAA's custody in order to prevent incidents like the Data Breach from reoccurring in the future. Given that information relating to the Data Breach, including the systems that were impacted, the configuration and design of Defendant's website, and the method of accessing PII in Defendant's insurance quoting process

remain exclusively in Defendant's control, Plaintiffs anticipate additional support for their claims will be uncovered following a reasonable opportunity for discovery.

PARTIES

A. Plaintiffs

20. Plaintiff Vincent Dolan ("Plaintiff Dolan") is a resident of Westchester County, New York. Plaintiff Dolan is not a member of the military and was not a member of USAA before Defendant allowed the creation of a fraudulent account in his name by unknown cyber criminals. Plaintiff Dolan's PII was disclosed without his authorization to unknown third parties as a result of USAA's Data Breach.

21. Since disclosing Plaintiff Dolan's PII, Plaintiff Dolan has personally experienced fraud. Immediately after the Data Brach, cyber criminals used his PII, which it obtained from USAA, to fraudulently file a claim for unemployment in his name.

22. Since the announcement of the Data Breach, Plaintiff Dolan has been required to spend his valuable time and resources in an effort to detect and prevent any additional misuses of his PII. Plaintiff Dolan would not have to undergo such time-consuming efforts but for the Data Breach.

23. As a result of the Data Breach, Plaintiff Dolan has been and will continue to be at heightened risk for fraud and identity theft, and its attendant damages for years to come. Such risk is real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach, and that this information was already illegally used by cyber criminals after the Data Breach to fraudulently file a claim for unemployment in the name of Plaintiff Dolan.

24. Plaintiff Christine Mapes ("Plaintiff Mapes") is a resident of Nassau County, New York. Plaintiff Mapes is not a member of the military and was not a member of USAA before Defendant allowed the creation of a fraudulent account in her name by unknown cyber criminals. Plaintiff Mapes' PII was disclosed without her authorization to unknown third parties as a result of USAA's Data Breach.

25. Since disclosing Plaintiff Mapes' PII, Plaintiff Mapes has personally experienced fraud. Immediately after the Data Brach, cyber criminals used her PII, which it obtained from USAA, to fraudulently obtain and take out an insurance policy in her name from another third-party provider.

26. Since the announcement of the Data Breach, Plaintiff Mapes has been required to spend her valuable time and resources in an effort to detect and prevent any additional misuses of her PII. Plaintiff Mapes would not have to undergo such time-consuming efforts but for the Data Breach.

27. As a result of the Data Breach, Plaintiff Mapes has been and will continue to be at heightened risk for fraud and identity theft, and its attendant damages for years to come. Such risk is real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach, and that this information was already illegally used by cyber criminals after the Data Breach to obtain an auto insurance policy through a third-party insurance provider in the name of Plaintiff Mapes.

B. Defendant

28. Defendant USAA is a reciprocal interinsurance exchange organized under Texas law and is an unincorporated association. Defendant USAA provides insurance and financial services, and its principal place of business is in San Antonio, Texas.

JURISDICTION AND VENUE

29. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States, including the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.*

30. Alternatively, the Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) because Plaintiffs and Defendant are citizens of different states and the amount in controversy exceeds $5,000,000.

31. The Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a) because the state law claims are related to claims in the action within such original jurisdiction and they form part of the same case or controversy under Article III of the United States Constitution.

32. This Court has personal jurisdiction over Defendant because (1) Defendant actively markets its products and conducts a substantial business in and throughout New York, where there are a considerable number of USAA members; (2) Defendant is registered with the New York State Department of Financial Services which regulates insurers in the state; and (3) the wrongful acts alleged in the Amended Complaint, including USAA's intentional disclosure of Plaintiffs' New York State Driver's License numbers, caused harm to Plaintiffs in New York.

33. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

A. The USAA Insurance Application Process

34. USAA offers insurance, banking, investment, retirement, and mortgage services. USAA proclaims that it "earned [their] members' trust by providing convenient banking and competitively priced insurance, and a comprehensive suite of investment products through [its] strategic providers."

35. USAA's products and services are only available to U.S. military members and veterans, pre-commissioned officers, spouses, and children.

36. To enjoy these benefits, an individual must first become a member of USAA.

37. When creating an account, USAA first will "check if [the individual] qualif[ies] for USAA membership." In checking to see if an individual qualifies, USAA will ask certain questions such as: "Have you served in the U.S. Armed Forces?" To get an auto insurance quote from USAA, users are asked the same qualifying questions.

38. Under USAA's current framework on its website, which it configured and designed, individuals seeking an insurance quote from USAA are only required to provide minimal information. The remainder of the information needed to process the request is typically obtained from the relevant state's department of motor vehicles ("DMV") or other third parties, such as insurers or data aggregators, who receive this information from state DMVs.

39. This is by design. USAA, like other insurers, intentionally allows individuals requesting a quote to provide only limited information. This is a benefit to USAA as it allows USAA to employ less workers and handle less phone calls from consumers.

40. In addition, this makes the process faster and less burdensome on the consumer, increasing the likelihood that they submit the application and thus increasing the number of

requests for quotes that USAA receives. However, this 'shortcut' process and intentional design feature on USAA's systems also makes it extremely ripe for exploitation and misuse by cyber criminals, such as what occurred to Plaintiffs and Class Members.

41. Upon information and belief, if a user receives an auto insurance quote from USAA, USAA discloses the user's Driver's License number on the quote.

42. However, this process of applying for an insurance quote is easily exploitable by cyber criminals to obtain the PII of other individuals, such as Plaintiffs and Class Members, who are not voluntary members of USAA.

43. For example, cyber criminals who possess only minimal and basic information of Plaintiffs and Class Members—such as a name, an address, and a date of birth, some of which may have been stolen or found elsewhere—can submit fraudulent requests for insurance quotes to extract more detailed and sensitive PII from USAA's system, such as Driver's License numbers, which USAA provides in response to the on-line request on the final insurance quote. By repeating this extraction process for multiple individuals, cyber criminals can develop a cache of highly sensitive personal information, including Driver's License numbers, that they can then use to commit fraud or identity theft or sell such PII on the dark web to other bad actors.

44. Plaintiffs and Class members are entitled to security of their PII. As an association collecting and storing sensitive information, and as DMV contractor with access to sensitive data such as Driver's License numbers, USAA has a duty to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

B. USAA Was on Notice that a Data Breach Was Likely

45. On February 16, 2021, the New York State Department of Financial Services ("NYSDFS") issued a cyber security fraud alert (the "February 2021 Cyber Fraud Alert")[1] to the Chief Executive Officers, Chief Information Officers, Chief Information Security Officers, Senior Information Officers, and Data Privacy Officers of all regulated entities, including Defendant.

46. The February 2021 Cyber Fraud Alert informed those entities that cyber criminals were exploiting cybersecurity flaws on websites to steal nonpublic information ("NPI"), specifically referencing 23 NYCRR § 500.01(g).

47. 23 NYCRR § 500.01(g)(2)(ii) defines NPI as "all electronic information that is not publicly available information and is: any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: drivers' license number or non-driver identification card number."

48. Specifically, the February 2021 Cyber Fraud Alert warned:

a. that cyber criminals were targeting "websites that offer instant online automobile insurance premium quotes . . . to steal unredacted driver's license numbers;"

b. "the activity appears to be part of an overall increase to steal NPI, driven in part by increase fraud activity during the pandemic;"

c. "this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits;" and

[1] A copy of the NYSDFS February 2021 Cyber Fraud Alert can be found at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_ednref1.

d. there were communications on "cybercrime forums offering to sell techniques to access driver's license numbers from auto insurance websites and step-by-step instruction on how to steal them."

49. In light of this criminal activity, NYSDFS warned that all websites who offer instant online automobile insurance premium quotes "are vulnerable to this type of data theft."

50. To prevent this type of data theft, the NYSDFS recommended that all regulated entities should "review whether it is necessary to display any NPI – even redacted to users, especially on public-facing websites. NPI should not be displayed on public-facing websites unless there is a compelling reason to do so."

51. NYSDFS further recommended that "[e]ntities that maintain any public-facing website that displays or transmits NPI should also take the following steps:"

- Conduct a thorough review of public-facing website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS) and Hypertext Markup Language (HTML) configurations;

- Review public-facing websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites;

- Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches the public-facing website;

- Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides;

- Search and scrub public code repositories for proprietary code; and

- Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.

52. On March 30, 2021, NYSDFS followed up with a second alert (the "March 2021 Cyber Fraud Alert Follow-Up") to the Chief Executive Officers, Chief Information Officers, Chief Information Security Officers, Senior Information Officers, and Data Privacy Officers of all regulated entities, including Defendant, concerning the exploitation of data pre-fill systems.[2]

53. In its March 2021 Cyber Fraud Alert Follow-Up, NYSDFS "**urge[d] personal lines insurers and other financial services companies to avoid displaying prefilled NPI on public-facing websites considering the serious risk of theft and consumer harm."** (Emphasis in the original).

54. The NYSDFS March 2021 Cyber Fraud Alert Follow-Up recommended that "[t]o combat this cybercrime, the following basic security steps should be implemented. Companies that continue to use Instant Quote Websites should also be prepared for cybercriminals to continue using new methods of attack," including:

- **Disable prefill of redacted NPI.** Avoid displaying prefilled NPI, especially on public-facing websites. *See* 23 NYCRR 500.09.

- **Install Web Application Firewall (WAF).** WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity. *See* 23 NYCRR 500.02(b)(2).

- **Implement CAPTCHA.** Cybercriminals use automated programs or "bots" to steal data. Completely Automated Public Turing Tests ("CAPTCHA") attempt to detect and block bots. *See* 23 NYCRR 500.02(b)(2).

- **Improve Access Controls for Agent Portals.** Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS's cybersecurity regulation. Measures that should be implemented include:
    - MFA, *see* 23 NYCRR 500.12;
    - Robust password policy, *see* 23 NYCRR 500.03 and 500.07; and
    - Limitations on login attempts, *see* 23 NYCRR 500.03 and 500.07.

[2] A copy of the NYSDFS March 2021 Cyber Fraud Alert Follow-Up can be found at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

- **Training and awareness.** Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls. *See* 23 NYCRR 500.14.

- **Limit access to NPI.** Employees and agents should only have access to sensitive information that is necessary to do their job. *See* 23 NYCRR 500.03(d) and 500.07.

- **Wait until payments have cleared before issuing a policy.** Auto insurers should consider waiting until an eCheck, credit card, or debit card payment has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI. *See* 23 NYCRR 500.02, 500.03, 500.07, and 500.09.

- **Protect NPI received from data vendors.** Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible from the internet or agent portals. *See* 23 NYCRR 500.02(b)(2) and 500.08.

55. Defendant USAA is an entity regulated by NYSDFS and received and/or had knowledge of the February 2021 Cyber Fraud Alert and the March 2021 Cyber Fraud Alert Follow-Up.

56. USAA did not follow NYSDFS's recommendations to secure Plaintiffs' and Class Members' PII.

57. USAA suffered the type of data breach that NYSDFS predicted and warned it about.

C. The Consent Orders Issued by the Comptroller of the Currency

58. On or around December 24, 2018, the Office of the Comptroller of the Currency ("OCC") entered into a Consent Order with USAA entitled *In the Matter of: USAA Federal Savings Bank San Antonio, Texas*, AA-EA-2018-90 (United States of America Department of the Treasury Office of the Comptroller of the Currency) ("Consent Order I").

59. Consent Order I focused on, among other things, USAA's failure "to implement and maintain an effective, comprehensive IT program" whereas "its IT program was not in compliance with the guidelines established in 12 C.F.R. Part 30, Appendix B."

60. Consent Order I states in relevant part:

* * *

ARTICLE VII

INFORMATION TECHNOLOGY

(1) Within sixty (60) days of receipt of a prior written determination of no supervisory objection to the Action Plan, the Bank shall perform an assessment of the Bank's IT Risk Governance Program and prepare a written report detailing the Bank's findings ("IT Assessment"). The IT Assessment shall include, but not be limited to, the Bank's compliance with 12 C.F.R. Part 30, Appendix B and safe and sound banking practices relating to IT, as well as identification of the skills and ***expertise needed to develop and maintain a compliant and safe and sound IT program*** and of any gaps with current staff. Refer to the FFIEC Information Technology Examination Handbook for additional guidance. Upon completion, a copy of the IT Assessment shall be provided to the Board or a designated committee thereof and to the Assistant Deputy Comptroller.

(2) Within sixty (60) days of completion of the IT Assessment, the Bank shall prepare and submit to the OCC, for written determination of no supervisory objection by the Assistant Deputy Comptroller, ***a written plan describing the actions necessary for the Bank to implement and maintain an effective IT Risk Governance Program, including specific timeframes for the development and implementation of the required corrective action ("IT Risk Governance Plan")***. In the event the Assistant Deputy Comptroller directs the Bank to revise the IT Risk Governance Plan, the Bank shall promptly make the necessary and appropriate revisions and submit the revised IT Risk Governance Plan to the Assistant Deputy Comptroller for review and written determination of no supervisory objection. Refer to the FFIEC Information Technology Examination Handbook for additional guidance. The IT Risk Governance Plan shall, at a minimum, include:

(a) an effective IT risk governance framework that establishes the roles, responsibilities, and accountability of front-line units and independent risk management;

(b) a program to develop, attract, and retain talent and maintain appropriate staffing levels to fulfill respective roles in the Bank's IT program;

(c) a program and methodology adhered to by front line units to assess, measure, and limit IT risks and concerns on an ongoing basis commensurate with the risk profile and risk appetite of the Bank;

(d) a program and methodology to assess, measure, aggregate, and limit IT risks and concerns on an ongoing basis commensurate with the risk profile and risk appetite of the Bank applicable to each of the three lines of defense, namely front line units, independent risk management, and internal audit, as described in 12 C.F.R. Part 30, Appendix D;

(e) an effective enterprise architecture;

(f) an information security program that complies with the requirements set forth in 12 C.F.R. Part 30, Appendix B;

(g) controls to ensure adherence to policies, procedures and processes;

(h) IT risk appetite metrics and limits;

(i) IT risk reporting and information systems;

(j) procedures for reporting and escalating significant IT risks and concerns and remediation activities to senior management and the Board; and

(k) a comprehensive training program for front line units, independent risk management, and internal audit personnel.

(3) Upon receipt of a determination of no supervisory objection from the Assistant Deputy Comptroller, the Board shall adopt the IT Risk Governance Plan and ensure management has timely implemented, and thereafter adheres to, the IT Risk Governance Plan. Prior to making any material changes to the IT Risk Governance Plan, the Bank shall submit a revised plan to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection. [Emphasis added].

61. On October 12, 2020, the OCC entered into a second Consent Order with USAA entitled *In the Matter of: USAA Federal Savings Bank San Antonio, Texas*, AA-ENF-2020-67 (United States of America Department of the Treasury Office of the Comptroller of the Currency) ("Consent Order II").

62. Consent Order II focused on, among other things, USAA's "unsafe or unsound banking practices relating to the Bank's compliance risk management program and information technology ("IT") risk governance program[.]"

63. Consent Order II states in relevant part:

[…] the OCC intends to initiate civil money penalty proceedings against the Bank pursuant to 12 U.S.C. § 1818(i), through the issuance of a Notice of Assessment of a Civil Money Penalty ***for engaging in unsafe or unsound practices related to the Bank's compliance risk management program and IT risk governance program that resulted in numerous violations of law***;

[…] in the interest of cooperation and to avoid additional costs associated with administrative and judicial proceedings with respect to the above matter, the Bank, by and through its duly elected and acting Board of Directors ("Board"), consents to the issuance of this Consent Order ("Order"), by the OCC through the duly authorized representative of the Comptroller of the Currency ("Comptroller");

***

(1) The Bank ***has failed to implement and maintain an effective compliance risk management program and an effective IT risk governance program commensurate with the Bank's size, complexity, and risk profile.*** The Bank has deficiencies in all three lines of defense (first-line business units, independent risk management, and internal audit) in its compliance risk management program.

***

The Bank shall make payment of a civil money penalty in the total amount of eighty-five million dollars ($85,000,000), which shall be paid upon the execution of this Order.

***

(1) This Order is a settlement of the civil money penalty proceeding against the Bank contemplated by the OCC, based on the unsafe or unsound practices ***resulting from the Bank's deficient compliance risk management program and IT risk governance program described in the Comptroller's Findings set forth in Article II of this Order***. This settlement includes civil money penalties for violations of laws or regulations pursuant to 12 U.S.C. § 1818(i) occurring prior to the date of this Order to the extent that (a) such past violations were caused by the Bank's deficient compliance risk management program or deficient IT risk governance program, and (b) such past violations have been identified or are identified by the Bank and remediated no later than December 31, 2021, pursuant to Article VI, paragraph (2) of the 2019 Order. [Emphasis added].

D. USAA's Chief Security Officer's Public Statements

64. On September 14, 2017, USAA's Chief Security Officer bragged about USAA's cyber security. In an article issued by *Forbes* entitled *Serving Those Who Have Served: Why Protecting Web Services Is Critical At USAA*, USAA's Chief Security Officer, Gary McAlum, stated:

> ***Any financial institution with millions of members across the globe faces significant cybersecurity challenges. As an exclusive provider to members of the U.S. military, USAA faces additional complexities that stem directly from its members' work in defending the country***.
>
> The Texas-based company provides banking, insurance and investment services to 12 million active and retired service members and their families. With military personnel deployed around the world, USAA is expected to deliver a fast and reliable online experience no matter where members are when they need to do business.
>
> Because many active service members have financial challenges, USAA strives to minimize anxiety over money matters by ensuring the lights are always on for members. That need is felt acutely across the organization.
>
> **Pressure On Military Members**
>
> Because availability is such a high priority, USAA makes all of its security decisions with uptime in mind.
>
> "***Since we are a digital organization, having always-on, always-connected service is critical for us***," said Gary McAlum, the chief security officer at USAA. "***We talk about the impact on member experience if there's a security failure, whether it affects one member or the membership as a whole***."
>
> ***McAlum is the company's first CSO***. Before taking the position seven years ago, he served 25 years in the U.S. Air Force, much of it in a cybersecurity role for the Department of Defense.
>
> At USAA, ***McAlum is responsible for defending the enterprise against all security, continuity and compliance threats — from massive cyberattacks to small-scale fraud***. When designing protections for USAA and its members, like a recent rollout of multifactor authentication, he considers what most members have already been through.

USAA knows that a large percentage of members were victims of a deep data breach*: *Over 20 million federal and military-connected individuals were affected by the attack on the U.S. Office of Personnel Management. The breach put personal information in the hands of criminals, information that could be used to exploit existing financial accounts or to fraudulently open new ones. McAlum and his family were among the many caught in that net.

"We tend to believe that our military members are more vulnerable to attack than others. There has always been a criminal aspect of society looking to scam and to exploit military members," he said. "So we focus a lot on education and awareness, including raising awareness of phishing attacks."

Withstanding Large-Scale Attacks

While fending off individual scammers, USAA must also stay secure and available in the face of a large, well-organized cyberattack. USAA was targeted by the Operation Ababil spree of distributed denial of service (DDoS) cyberattacks against U.S.-based financial institutions in 2012 to 2013.

USAA had advance notice of the planned attack. After assessing the network infrastructure provided by Akamai, USAA felt confident that the planned attack would not disrupt member services. That prediction proved correct. Akamai protections deflected much of the traffic that might have otherwise overwhelmed crucial services.

DDoS attacks often target the independent domain name servers (DNS) that resolve domain names, like USAA.com, to hosting servers. Overwhelm the DNS, and legitimate traffic can't find a business. Distributing DNS across Akamai's wide network helps protect against that threat.

"Both of the scheduled attack days were nonevents for us. We saw an activity spike, and then saw it dissipate," McAlum said. "Akamai's network gives us a very wide front door and was able to dissipate that DDoS attack very easily."

How Executive Culture Affects Security

Considering that any security chief needs strong alignment with other executives, USAA designed the CSO office to be fully independent, with a close link to senior leaders at the top.

"***We wanted one budget, one line of accountability for security***," he said. "Today, everything from security to investigations to business continuation falls under the security group I lead."

> At USAA, the CIO and CSO are peers on the organizational chart. Instead of struggling to find common ground, the two have a great deal in common, McAlum said.
>
> "The culture of our company, driven from the board of directors down, is that we have to be available to our members," he said.
>
> The partnership is working: USAA conducts an estimated 1.4 billion digital transactions each year and continues to avoid major incident.
>
> Against a steady drumbeat of high-profile data breaches, McAlum said he considers the company's stability and unique CSO-CIO partnership as a model for others.
>
> "We will continue to work very closely with the CIO side of the house, because we all understand that if our products and services are not available or compromised, nobody wins," he said. [Emphasis added].

65. Despite USAA's CSO's lofty statements regarding cybersecurity in 2017, USAA's configuration and design of its own systems that resulted in the Data Breach proved otherwise.

E. The USAA Data Breach

66. On June 2, 2021, USAA notified Plaintiffs and claimed that "Fraudsters . . . gain[ed] unauthorized access to your driver's license number through the auto insurance quote process on our website." USAA admitted "[y]our driver's license number was accessed in this incident. When combined with other personal information a driver's license number can be used for purposes such as filing fraudulent unemployment claims."

67. The PII these cyber criminals intentionally obtained through USAA from Plaintiffs has already been used for fraudulent activity by way of obtaining an auto insurance policy through an unrelated third-party insurance provider (as to Plaintiff Mapes) and filing a fraudulent claim for unemployment benefits (as to Plaintiff Dolan).

68. Further, the information disclosed by Defendant has also been used to file fraudulent unemployment claims on behalf of other Class Members.

69. As these cyber criminals have already used the PII compromised in the Data Breach to commit financial fraud and identity theft, Plaintiffs and Class Members have been and remain at an imminent risk of future fraud and identity theft.

F. USAA Obtains, Collects, and Stores Plaintiffs' and Class Members' PII

70. In the ordinary course of doing business as an automobile insurer, USAA regularly requires its members to provide their sensitive, personal, and private protected information in order to register and use Defendant's services.

71. Additionally, automobile insurers, such as USAA, also store and obtain additional personal information that they receive from other sources. For instance, automobile insurers share claims information among themselves to help weed out consumers who switch to other providers. These insurers also have access to a consumer's Driver's License number, current auto policy data, and make and model of a consumer's vehicle. Often, this information needed to process the request is typically obtained from the relevant state DMVs or other third parties, such as insurers or data aggregators, who receive this information from state DMVs.

72. As an automobile insurer, USAA purposefully aims to make applying for a policy as easy as possible in order to attract new customers and increase its business. To do so, USAA only requires a minimal amount of information to apply for a policy. The remainder of the information is filled in from data acquired from other sources.

73. Cyber criminals employ a variety of techniques for obtaining this PII, including extracting data from the website's code, using web developer tools meant for debugging, and calling live agents with enough other information to persuade them to hand over other forms of personal information, such as Driver's License numbers. Indeed, the practice is so prominent there are 'how-to guides' that aspiring criminals can buy that have appeared on cybercrime forums.

74. But USAA did not have to configure or design its systems in this way. For example, instead of auto populating insurance quote fields with highly sensitive PII, Defendant could have validated the user's information and processed the quote on the 'back-end' after receiving the applicant's information. Nor was there a need for Defendant to disclose highly sensitive PII, like a purported applicant's Driver's License number in response to a request for a quote.

75. USAA is in complete operation, control, and supervision of its website and systems, including the insurance quote portal. Defendant intentionally configured and designed its website and systems this way because it helped to increase the number of quotes requested, benefiting its business, without regard to Plaintiffs' and Class Members' PII which was disclosed to cyber criminals in the process given this exploitability.

76. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, USAA assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

77. Thus, USAA had access to Plaintiffs' and Class Members' PII, including their Driver's License Numbers, which was stored on their systems, which it then intentionally disclosed when generating a quote.

78. Plaintiffs and Class Members reasonably expect that insurance service providers such as Defendant will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

79. Defendant acknowledges that it has an obligation to protect PII from disclosure. Defendant states on its website that "If you are a member and your Personal Information is

'nonpublic personal information' that we collect in connection with providing you a financial product or service, your Personal Information is . . . protected by our Privacy Promise."

80. Though Plaintiffs did not sign up for USAA on their own, they were nonetheless involuntary "members" of the system once cyber criminals used their information to fraudulently create an account. USAA, by its own admission, therefore, owed Plaintiffs the same duty to protect their PII as other members.

81. Defendant's "Privacy Promise" states that it promises not to "sell your information" and take certain measures to "protect your information."

82. Despite Defendant's commitment to protecting personal information, USAA failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

83. Had USAA remedied the security deficiencies, heeded advice from government regulators, followed industry guidelines, and adopted security measures recommended by experts in the field, USAA would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

G. The Value of Private Information and Effects of Unauthorized Disclosure

84. USAA was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

85. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale

and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cyber criminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

86. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud." PII is valued on the dark web at approximately $1 per line of information.

87. Driver's License numbers in particular—which were compromised as a result of the Data Breach—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive.

88. *Experian*, a globally recognized credit reporting agency, has explained "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves." This is because a Driver's License number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, NY Department of Taxation and Finance and other government agencies, places of employment, doctor's offices, and other entities.

89. For these reasons, Driver's License numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

90. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique Driver's License numbers—cannot be easily replaced.

91. The ramifications of USAA's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

92. Thus, USAA knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. USAA failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

H. FTC Guidelines, NY Shield Act, and the DPPA

93. USAA is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

94. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

95. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

96. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

97. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

98. USAA failed to properly implement basic data security practices. USAA's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Driver's License information provided in its response to requests for insurance quotes, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

99. USAA was at all times fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. USAA was also aware of the significant repercussions that would result from its failure to do so.

100. Defendant also had an obligation to use reasonable security measures under New York's Shield Act (N.Y. Gen. Bus. Law § 899-aa, *et seq.* (known as the "NY Shield Act"), which

requires businesses that collect private information to implement reasonable cybersecurity safeguards to protect that information.

101. The NY Shield Act also mandates the implementation of a data security program, including measures such as risk assessments, workforce training and incident response planning and testing, and became effective on or about March 21, 2020.

102. Defendant also had an obligation under the DPPA. The DPPA was enacted in 1994 in response to safety and privacy concerns stemming from the ready availability of personal information contained in state motor vehicle records. The DPPA was passed in the backdrop of the murder of actress Rebecca Schaeffer, whose murderer obtained her unlisted address through the California Department of Motor Vehicle (DMV). Additional concerns were raised when witnesses testified in hearings before Congress regarding the privacy of DMV information of domestic violence victims and law enforcement officers, among other safety concerns surrounding driver information. To address these concerns, the DPPA restricts the disclosure of personal information from motor vehicle records to certain permissible purposes expressly defined by the act.

103. The unauthorized disclosures of information have long been seen as injurious. The common law alone will sometimes protect a person's right to prevent the dissemination of private information. Indeed, it has been said that privacy torts have become well-ensconced in the fabric of American law. And with privacy torts, improper dissemination of information can itself constitute a cognizable injury. Because damages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable, causes of action such as the DPPA provide privacy tort victims with a monetary award calculated without the need of proving actual damages.

104. The DPPA states that "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1).

105. Defendant had an obligation to use reasonable security measures under the DPPA, which further states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

106. Thus, the DPPA provides citizens with a private right of action in the event that their private information is knowingly obtained, disclosed, or used in a manner other than for the enumerated permissible purposes. The DPPA states: "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter [18 U.S.C. §§ 2721, *et seq*.] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724(a).

107. The default rule under the DPPA is non-disclosure. The DPPA is structured such that 18 U.S.C. § 2721(a)(1) and 18 U.S.C. § 2722(a) provide the general prohibition on the release and use of motor vehicle information, and § 2721(b) enumerates fourteen specific exceptions to the general prohibition. Disclosing information to cyber criminals is not one of them. Because the PII was disclosed to unauthorized individuals—*i.e.*, cyber criminals—there is no argument to be made that disclosure was "for a permissible purpose."

I. Plaintiffs and Class Members Suffered Damages

108. The ramifications of USAA's failure to keep PII secure are long lasting and severe. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

109. Plaintiffs and Class Members have faced an actual as well as substantial and imminent risk of identity theft and fraud as a result of the Data Breach. Unauthorized individuals carried out the Data Breach and stole the personal information of Plaintiffs and Class Members with the intent to use it for fraudulent purposes and/or sell it to other cyber criminals. This is confirmed, as the cyber criminals who compromised Plaintiffs' PII have already used Plaintiffs' PII to commit fraud by way of obtaining an auto insurance policy through an unrelated third-party insurance provider (as to Plaintiff Mapes) and filing a fraudulent claim for unemployment benefits (as to Plaintiff Dolan). Indeed, the Data Breach notice USAA sent to Plaintiffs also admits fraudulent unemployment claims are one of the potential identity theft risks caused by the unauthorized discovery of a person's Driver's License number.

110. The risk of identity theft is particularly substantial when the PII compromised, in this instance Driver's License numbers, is unique to a specific individual and extremely sensitive.

111. Plaintiffs and Class Members have already spent and will spend substantial amounts of time monitoring their accounts for identity theft and fraud and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

112. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

113. Further, many Class Members will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

114. Besides the monetary damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

115. Despite all of the publicly available knowledge of the continued compromises of PII and the importance of securing such information, USAA's commitment to privacy fell by the wayside. Rather than protect Plaintiffs' and Class Members' PII, USAA ignored these risks and knowingly configured and designed its systems in a way that disclosed this information to cyber criminals.

116. As an auto insurance company that handles personal information containing Driver's License numbers as part of its business model, USAA was well aware of the requirements and purpose of the DPPA.

117. As an entity that receives information obtained from state DMVs, USAA was well-informed that the PII it collected was highly sensitive personal data, and that disclosure of that information to the public by, for example, storing it on systems accessible to the whole internet, would violate the DPPA.

118. Critically, only USAA had control over the configuration and design of its own systems, and knowingly chose to forego the necessary data protection techniques needed for it to secure Plaintiffs' and Class Members' PII.

119. Despite the clear dangers that the insecure use of PII poses, USAA knowingly chose to configure and design its systems to disclose Plaintiffs' and Class Members' PII to unauthorized third parties.

120. As a result of USAA's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the actual, imminent, and certainly impeding injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cyber criminals; damages to and diminution in value of their PII; and continued risk to Plaintiffs' and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

121. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide class:

> All individuals in the United States whose PII was disclosed on auto insurance quotes or policies by USAA to unauthorized third parties.

122. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded

party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

123. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

124. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. According to the Bureau of Internet & Technology of the State of New York Office of Attorney General, the Data Breach affected approximately 22,383 individuals, including approxinately 12,627 New York State residents. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court.

125. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

126. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant was negligent in collecting and disclosing Plaintiffs' and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

f. Whether Defendant breached their duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII by disclosing that information on insurance quotes in the manner alleged herein, including failing to comply with industry and governmental regulator standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant intentionally configured and designed its online system to benefit its business in such a way that it foreseeably allowed unauthorized persons and/or cyber criminals to gain access to the PII of Plaintiffs and Class Members;

i. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

k. Whether Defendant violated 18 U.S.C. §§ 2721, *et seq.*, by disclosing Plaintiffs' and Class Members' PII;

l. Whether Defendant violated New York General Business Law, § 349, *et seq.*;

m. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

127. The requirements of Rule 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of Class Members. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiffs and Class Members each had their PII disclosed by USAA to an unauthorized third party.

128. The requirements of Rule 23(a)(4) are satisfied. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiffs and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

129. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

130. USAA owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

131. More specifically, this duty included, among other things: (a) designing, maintaining, and testing USAA's systems, including its website, to ensure that Plaintiffs' and Class Members' PII in USAA's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; (d) maintaining data security measures consistent with industry and governmental regulator standards; and (e) ensuring that USAA's systems did not disclose Plaintiffs' or Class Members' PII to unauthorized third-parties who fraudulently submitted requests for insurance quotes.

132. USAA's duty to use reasonable care arose from several sources, including but not limited to those described below.

133. USAA had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and disclosing valuable PII

that is routinely targeted by criminals for unauthorized access, USAA was obligated to act with reasonable care to protect against these foreseeable threats.

134. USAA admits that it has a duty to protect consumer data. *See* ¶ 79 *supra*.

135. USAA had a duty not to engage in conduct that creates a foreseeable risk of harm to Plaintiffs and Class Members.

136. USAA breached the duties owed to Plaintiffs and Class Members and thus was negligent. Specifically, USAA breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) design its on-line systems to prevent unauthorized users from making Plaintiffs and Class Member involuntary members of USAA and then extracting PII from USAA's on-line system; (c) detect the breach while it was ongoing; (d) maintain security systems consistent with industry and governmental regulator standards; and (e) disclose that Plaintiffs' and Class Members' PII in USAA's possession had been or was reasonably believed to have been, stolen or compromised.

137. But for USAA's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

138. As a direct and proximate result of USAA's negligence, Plaintiffs and Class Members have suffered injuries, including:

(a) Actual fraud;

(b) Theft of their PII;

(c) Diminution in value of their PII;

(d) Costs associated with requested credit freezes;

(e) Costs associated with the detection and prevention of identity theft;

(f) Costs associated with purchasing credit monitoring and identity theft protection services;

(g) Lowered credit scores resulting from credit inquiries following fraudulent activities;

(h) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the USAA Data Breach;

(i) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being disclosed to cyber criminals;

(j) Damages to and diminution in value of their PII entrusted, directly or indirectly, to USAA with the societal understanding that USAA would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

(k) Continued risk of exposure to hackers and thieves of their PII, which remains in USAA's possession and is subject to further breaches so long as USAA fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

139. As a direct and proximate result of USAA's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*

140. Plaintiffs restate and reallege all proceeding factual allegations above as if fully set forth herein.

Negligence *Per Se* Under Section 5 of the FTC Act

141. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as USAA for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of USAA's duty.

142. USAA violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards, including, disclosing full Driver's License numbers in plain text in response to requests for insurance quotes and configuring and designing its website to speed up the application process by auto populating quote fields at the risk of disclosing Plaintiffs' and Class Members' highly sensitive data. USAA's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

143. USAA's violation of Section 5 of the FTC Act constitutes negligence *per se*.

144. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

145. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

146. As a direct and proximate result of USAA's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Negligence *Per Se* Under the DPPA

147. The DPPA states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

148. The DPPA also states that "[a] State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1).

149. As alleged herein, USAA utilizes PII obtained from motor vehicle records, including Driver's License numbers, in connection with processing insurance applications.

150. Under the DPPA, USAA owed a duty to Plaintiffs and other Class Members to protect and not disclose their PII, including Driver's License numbers, obtained from motor vehicle records.

151. USAA violated the DPPA by intentionally configuring and designing its insurance quote application portal on its website to disclose Plaintiffs' and Class Members' PII to anyone who requested an insurance quote. USAA installed no protections or security measures to protect this information and willfully disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal. USAA's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

152. Alternatively, USAA had constructive notice that it had disclosed the PII of Plaintiffs and Class Members to unauthorized third parties, because it should have been aware that

configuring and designing its website to disclose Plaintiffs' and Class Members' PII to anyone who submitted a request for a quote without authentication or other security protections would cause the disclosure of this information.

153. At the very least, USAA was willfully ignorant that its website, servers, and systems were configured without any protections to store Plaintiffs' and Class Members' PII and would disclose that personal information to cyber criminals.

154. USAA's violation of the DPPA constitutes negligence *per se*.

155. Plaintiffs and Class Members are within the class of persons that the DPPA was intended to protect against because the DPPA was expressly designed to protect a person's personal information contained in motor vehicle records from unauthorized disclosure.

156. Moreover, the harm that has occurred is the type of harm the DPAA is intended to guard against, *i.e.*, the unauthorized disclosure of personal information from motor vehicle records.

157. As a direct and proximate result of USAA's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Negligence *Per Se* Under the NY Shield Act, N.Y. Gen. Bus. Law § 899-aa, *et seq.*

158. Under N.Y. Gen. Bus. Law § 899-bb(2)(a) "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

159. "Private information" is defined as "personal information" in combination with at least one other data element defined in N.Y. Gen. Bus. Law § 899-aa(1)(b), such as driver's license numbers.

160. "Personal information" is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." N.Y. Gen. Bus. Law § 899-aa(1)(a).

161. USAA owns or licenses computerized data that includes the private information, (*i.e.*, names and driver's license numbers) of New York residents, including Plaintiffs. As such, USAA was required to implement and maintain "reasonable safeguards" to protect this information.

162. Pursuant to N.Y. Gen. Bus. Law § 899-bb(2)(b), *et seq*., USAA was required to implement a "data security program" that includes reasonable "administrative" "technical" and "physical safeguards."

163. Reasonable administrative safeguards that USAA should have, but did not undertake, include: (a) designating one or more employees to coordinate a security program; (b) identifying reasonably foreseeable internal and external risks; (c) assessing the sufficiency of safeguards in place to control the identified risks; (d) training and managing employees in the security program practices and procedures; (e) selecting service providers capable of maintaining appropriate safeguards, requiring those safeguards by contract; and (f) adjusting the security program in light of business changes or new circumstances.

164. Reasonable technical safeguards that USAA should have, but did not, undertake include: (a) assessing risks in network and software design; (b) assessing risks in information processing, transmission, and storage; (c) detecting, preventing, and responding to attacks or system failures; and (d) regularly testing and monitoring the effectiveness of key controls, systems, and procedures.

165. Reasonable physical safeguards that USAA should have, but did not, undertake include: (a) assessing risks of information storage and disposal; (b) protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (c) disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

166. USAA breached its duties to Plaintiffs and Class Members under the NY Shield Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' private information and personal information.

167. USAA's violation of the NY Shield Act constitutes negligence *per se*.

168. Plaintiffs and Class Members are within the class of persons that the NY Shield Act was intended to protect because the NY Shield Act was expressly designed to protect New York residents' private and personal information.

169. The harm that has occurred is the type of harm the NY Shield Act is intended to guard against. Indeed, the entire purpose of the NY Shield Act is to prevent the occurrence of data breaches, like the USAA Data Breach, which put consumers' PII at risk.

170. But for USAA's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured, or would not have been injured to as great a degree.

171. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of USAA's breach of its duties. USAA knew or should have known that a breach of its duties would cause Plaintiffs and Class Members to suffer foreseeable harm associated with the exposure of their private information and personal information.

172. As a direct and proximate result of USAA's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

173. Whether under the FTC Act, the DPPA, or the NY Shield Act, each independently constitutes negligence *per se*.

COUNT III
VIOLATION OF 18 U.S.C. §§ 2721, *et seq.* (DPPA)

174. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

175. Pursuant to 18 U.S.C. § 2722(a), "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title."

176. Pursuant to 18 U.S.C. § 2721(a)(1), "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section."

177. The DPPA provides a civil cause of action against "a person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted" under the statute. 18 U.S.C. § 2724(a).

178. "Person" is defined as "an individual, organization or entity." 18 U.S.C. § 2725(2). USAA is a "person" under the DPPA.

179. "Personal information" is defined as "information that identifies an individual, including an individual's . . . driver identification number. . ." 18 U.S.C. § 2725(3). Plaintiffs' and

Class Members' PII, which includes Driver's License numbers, is "personal information" under the DPPA.

180. "Motor vehicle record" is defined as "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). USAA obtains motor vehicle records containing Plaintiffs' and Class Members' PII, including their Driver's License numbers.

181. USAA obtains motor vehicle records as part of its business operations intended to generate online insurance quotes and/or insurance policy processing for profit.

182. USAA's disclosure of Plaintiffs' and Class Members' personal information to unauthorized individuals violated 18 U.S.C. §§ 2722(a) and/or 2721(a)(1).

183. USAA's disclosure of personal information was not a permitted use under 18 U.S.C. § 2721(b).

184. USAA knowingly obtained and/or disclosed Plaintiffs' and Class Member's personal information, which came from a motor vehicle record, for a purpose not permitted under the DPPA.

185. USAA knowingly and voluntarily configured and designed its insurance quote application portal on its website to disclose Plaintiffs' and Class Members' PII to anyone who requested an insurance quote, all in direct violation of the DPPA.

186. USAA installed no protections or security measures to protect this exposed information and willfully disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal.

187. Alternatively, USAA had constructive notice that it had disclosed the PII of Plaintiffs and Class Members to unauthorized third parties, because it should have been aware that

configuring and designing its website to disclose Plaintiffs' and Class Members' PII to anyone who submitted a request for a quote without authentication or other security protections would cause the disclosure of this information.

188. Further, USAA was on notice of the February 2021 Cyber Fraud Alert and March 2021 Cyber Fraud Alert Follow-Up which informed USAA that cyber criminals were exploiting cybersecurity flaws on automobile insurance websites who offer instant online automobile insurance premium quotes by stealing nonpublic information, including Driver's License numbers.

189. At the very least, USAA was willfully ignorant that its website, servers, and systems were configured and designed without any protections to store Plaintiffs' and Class Members' PII and would disclose that personal information to cyber criminals.

190. Merriam-Webster's dictionary defines "disclose" as "to make known or public," "to expose to view," or, alternatively, "to open up." None of these definitions requires an identified intended recipient. Instead, disclosure is the act of exposure. Whether or not USAA meant for identifiable third parties to access the information is not relevant. All that is required for a knowing disclosure is a voluntary action.

191. Pursuant to 18 U.S.C. § 2724(b)(1)-(4), Plaintiffs seek, on behalf of themselves and members of the Class (1) actual damages, not less than statutory liquidated damages in the amount of $2,500; (2) punitive damages; (3) reasonable attorneys' fees and costs; and (4) preliminary and equitable relief as the Court determines to be appropriate.

COUNT IV
NEW YORK GENERAL BUSINESS LAW, N.Y. GEN. BUS. LAW § 349, *et seq.*

192. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

193. New York General Business Law § 349 ("§ 349") prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." § 349(a).

194. Plaintiffs and Class Members are "person[s]" within the meaning of § 349.

195. Plaintiffs are authorized to bring a private action under § 349(h).

196. Defendant USAA conducts business and provides its services, including auto insurance quotes and policies, in the State of New York.

197. In the conduct of their business, trade, and commerce, and in furnishing services in the State of New York, Defendant's actions were directed at consumers.

198. In the conduct of their business, trade, and commerce, and in furnishing services in the State of New York, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of § 349(a), including but not limited to, the following:

(a) Collecting, storing, and/or gaining access to Plaintiffs' and Class Members' PII without their knowledge or consent;

(b) Failing to disclose to Plaintiffs' and Class members that it would collect, store, and/or gain access to their PII;

(c) Failing to disclose to Plaintiffs' and Class members that it would disclose their PII without their knowledge or consent;

(d) Failing to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of Plaintiffs' and Class Members' PII, and omitting, suppressing, and concealing the material fact of that failure;

(e) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and omitting, suppressing, and concealing the material fact of that failure;

(f) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

(g) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(h) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII;

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

(j) Failure to comply with the NY Shield Act as a *per se* violation of N.Y. Gen. Bus. Law § 899-bb(2)(d).

199. Defendant systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and Class Members.

200. Defendant willfully engaged in such acts and practices and knew that they violated § 349 or showed reckless disregard for whether they violated § 349.

201. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

202. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

203. Defendant knew or should have known that the online system it configured and designed, its data security practices, and its unauthorized disclosures were inadequate to safeguard Class Members' PII and that therefore the risk of data breach or PII disclosures to unauthorized third parties was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless.

204. Plaintiffs and Class Members seek relief under § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF

205. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

206. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

207. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether USAA is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that USAA's data security measures remain inadequate.

USAA publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes USAA has undertaken in response to the Data Breach.

208. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. USAA owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, the NY Shield Act, and the DPPA;

b. USAA continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. USAA' ongoing breaches of its legal duty continue to cause Plaintiffs harm.

209. This Court also should issue corresponding prospective injunctive relief requiring USAA to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct USAA to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

210. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at USAA. The risk of another such breach is real, immediate, and substantial. If another breach at USAA occurs, Plaintiffs will not

have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

211. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to USAA if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to USAA of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and USAA has a pre-existing legal obligation to employ such measures.

212. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at USAA, thus eliminating the additional injuries that would result to Plaintiffs and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representative of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(c) For damages in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgment interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: January 31, 2022

Respectfully submitted,

GAINEY McKENNA & EGLESTON

By: */s/ Thomas J. McKenna*
Thomas J. McKenna
Gregory M. Egleston
501 Fifth Avenue, 19th Floor
New York, NY 10017
Telephone: (212) 983-1300
Facsimile: (212) 983-0383
Email: tjmckenna@gme-law.com
Email: gegleston@gme-law.com

LOWEY DANNENBERG, P.C.
Christian Levis
Amanda Fiorilla
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: clevis@lowey.com
Email: afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina (*pro hac vice*)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

LYNCH CARPENTER, LLP
Gary F. Lynch
Kelly K. Iverson (*pro hac vice* forthcoming)
Nicholas A. Colella (*pro hac vice*)
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243

Email: Gary@lcllp.com
Email: Kelly@lcllp.com
Email: NickC@lcllp.com

Co-Lead Interim Class Counsel for Plaintiffs and the Proposed Class